Use Case

Automating Security Policies Security Management

Modern Problems: Manual Security Access Changes

- A large financial services company had been afflicted by a common enterprise-grade ailment: inability to update security policies on time. Customer access to secure and confidential data was being hampered by the speed at which the access could be manually provided by the SecOps team. This slow access to data led to customer issues on making business decisions and questions of whether the service was worthwhile.

- This manual processing of requests led to backed up request logs, where a new request would take upwards of 4 hours to satisfy, at which time the request would no longer be relevant leaving a disgruntled customer.

- The companies question became, how can we automate the CRUD (Create, Read, Update and Delete) operations for the security policies while maintaining our existing tools and policies.

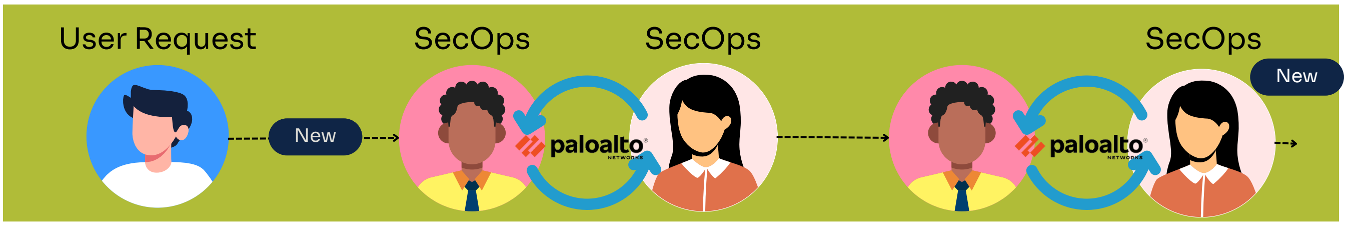
Composer Benefits

Cross-domain adaptation mimicking existing business process so there is no disruption with existing security tools

Updated financial information in seconds satisfying customer access to their data

Automating manual error prone tasks for more efficiency and security

The Conventional Manual Workflow Problem



A user request to update their security policy leads to a ServiceNow ticket being created with an existing selected policy to manually change. →

The SecOps team members now manually go through entering the changes that were selected to update policies, while hoping they have not been updated incorrectly. →

SecOps team members go through the commit and push phases of deployment for each device group specified, then a final check to ensure the new policies are updated. Then, the ServiceNow record is now updated and closed.

Manual Process: 3-4 Hours for Each Operation With Possible Manual Errors

FIGURE 1: Previous Manual Security Policy Update

Use Case

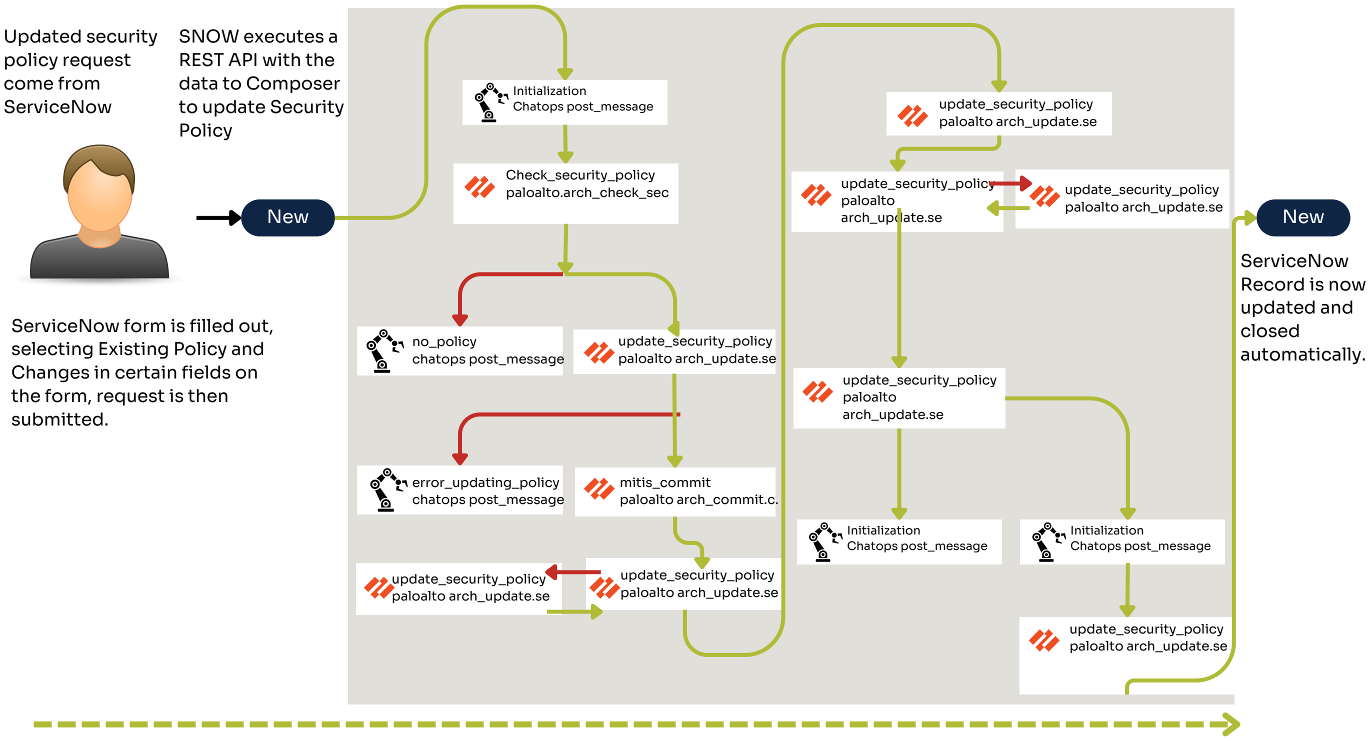
Automating Security Policies Security Management

Orchestral.ai's Composer Solution

In addressing this solution, the Orchestral.ai team was able to scope out the existing process, comply with all existing customer integrations including the ServiceNow ticketing system and pinpoint precisely which elements would be automated. Utilizing Composer's Palo Alto security pack Orchestral.ai was able to orchestrate on-demand access to any secure data and remove access after a specified time frame.

With Composer's flexibility to interact with both ServiceNow and Panorama, nothing needed to change from the existing tools and policies, instead the CRUD operations for the security policy updates were automated via the Composer workflow engine.

An end-to-end SecOps solution was written with the ability to orchestrate all CRUD operations for new or existing security policies. In doing so, Orchestral provided the Day 0, 1, and Day N phases of operation for the company's new secured network.



Composer checks all actions and updates the policy on Panorama, and then commits and pushes it to each device group specified.

Updated security policy request come from ServiceNow

SNOW executes a REST API with the data to Composer to update Security Policy

ServiceNow form is filled out, selecting Existing Policy and Changes in certain fields on the form, request is then submitted.

ServiceNow Record is now updated and closed automatically.

Composer: < 1 Minute of 100% Accurate Entries

FIGURE 2: Composer Automated Security Policy Update

Orchestral.ai

Conquer Complexity in Enterprise IT

Orchestral.ai is a team of like-minded technology professionals possessing a combined experience of over 100 years in the IT industry.

Contact Us: For more information, please contact our Client Development Team at info@orchestral.ai

About Us

Orchestral's mission is to enable IT infrastructure & operations teams to more effectively manage the complex mission critical processes that their organizations depend upon for day-to-day operations. We accomplish this today with the Orchestral Platform - an integrated suite of automation, orchestration and Explainable Artificial Intelligence (XAI) technologies designed to empower enterprises to start their transition toward Autonomous IT Infrastructure.

Visit: www.orchestral.ai